

Exponential notation	Quaternary polynomial notation	Binary polynomial notation of $GF(16)$ on $GF(2)$	Hexadecimal notation
0	0	0	0
α^0	1	1	1
α^1	X	x	2
α^2	x+2	x^2	4
α^3	3x+2	x^3	8
α^4	x+1	x+1	3
α^5	2	x^2+x	6
α^6	2x	x^3+x^2	C
α^7	2x+3	x^3+x+1	B
α^8	x+3	x^2+1	5
α^9	2x+2	x^3+x	A
α^{10}	3	x^2+x+1	7
α^{11}	3x	x^3+x^2+x	E
α^{12}	3x+1	x^3+x^2+x+1	F
α^{13}	2x+1	x^3+x^2+1	D
α^{14}	3x+3	x^3+1	9

Table I

Fig. 1

Exponential notation	Binary polynomial notation of $GF(4)$ on $GF(2)$	Quaternary notation
0	0	0
α^0	1	1
α^1	X	2
α^2	X+1	3

Table II

Fig. 2

Exponential notation	Quaternary polynomial notation	Binary polynomial notation	Hexadecimal notation
0	0	0	0
α^0	1	1	1
α^1	X	x	2
α^2	X+2	x^2	4
α^3	3x+2	x^3	8
α^4	X+1	x^3+1	9
α^5	2	x^3+x+1	B
α^6	2x	x^3+x^2+x+1	F
α^7	2x+3	x^2+x+1	7
α^8	X+3	x^3+x^2+x	E
α^9	2x+2	x^2+1	5
α^{10}	3	x^3+x	A
α^{11}	3x	x^3+x^2+1	D
α^{12}	3x+1	x+1	3
α^{13}	2x+1	x^2+x	6
α^{14}	3x+3	x^3+x^2	C

Table III

Fig. 3

Figure 4a and 4b show the structure of the H_{max} and H_{min} blocks, respectively. The inputs are $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ and the outputs are $\gamma_0, \gamma_1, \gamma_2, \gamma_3$.

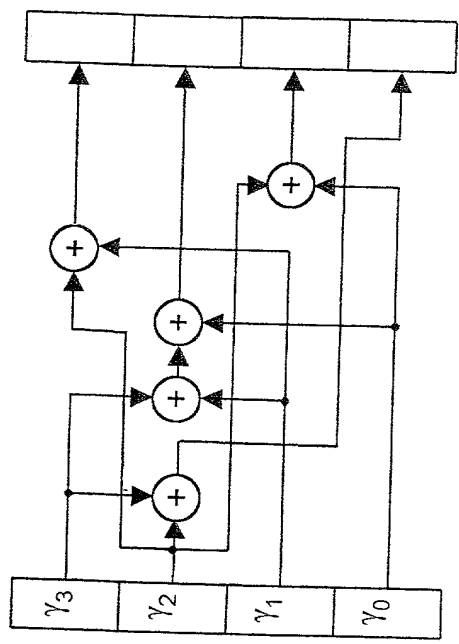


Fig. 4a

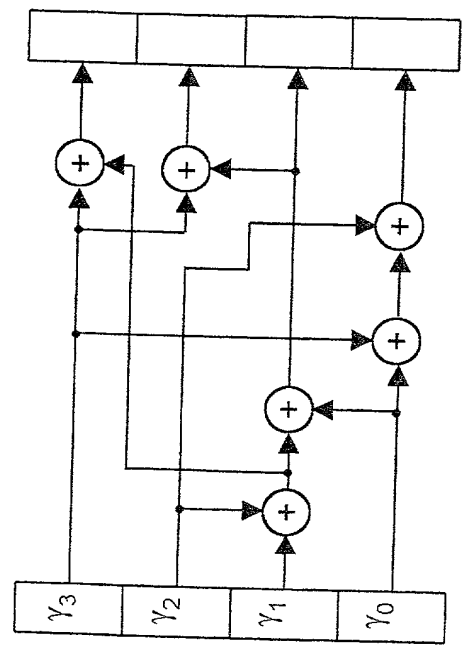


Fig. 4b

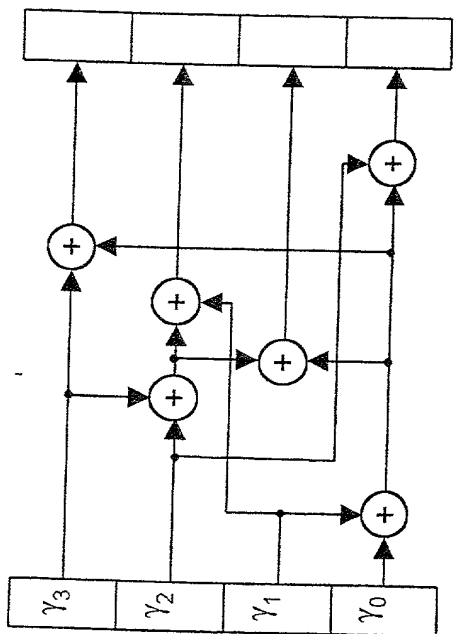


Fig. 5a

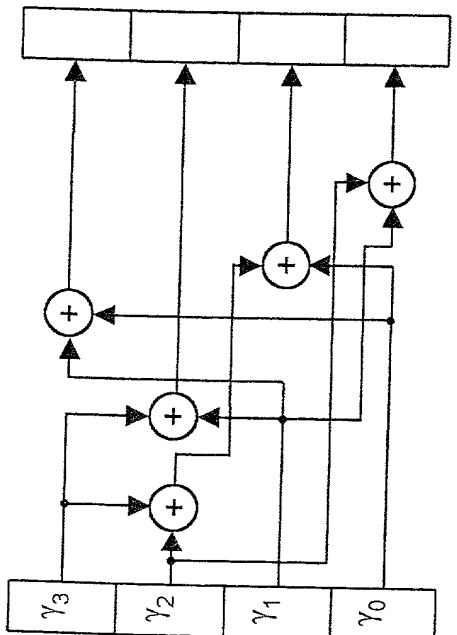


Fig. 5b

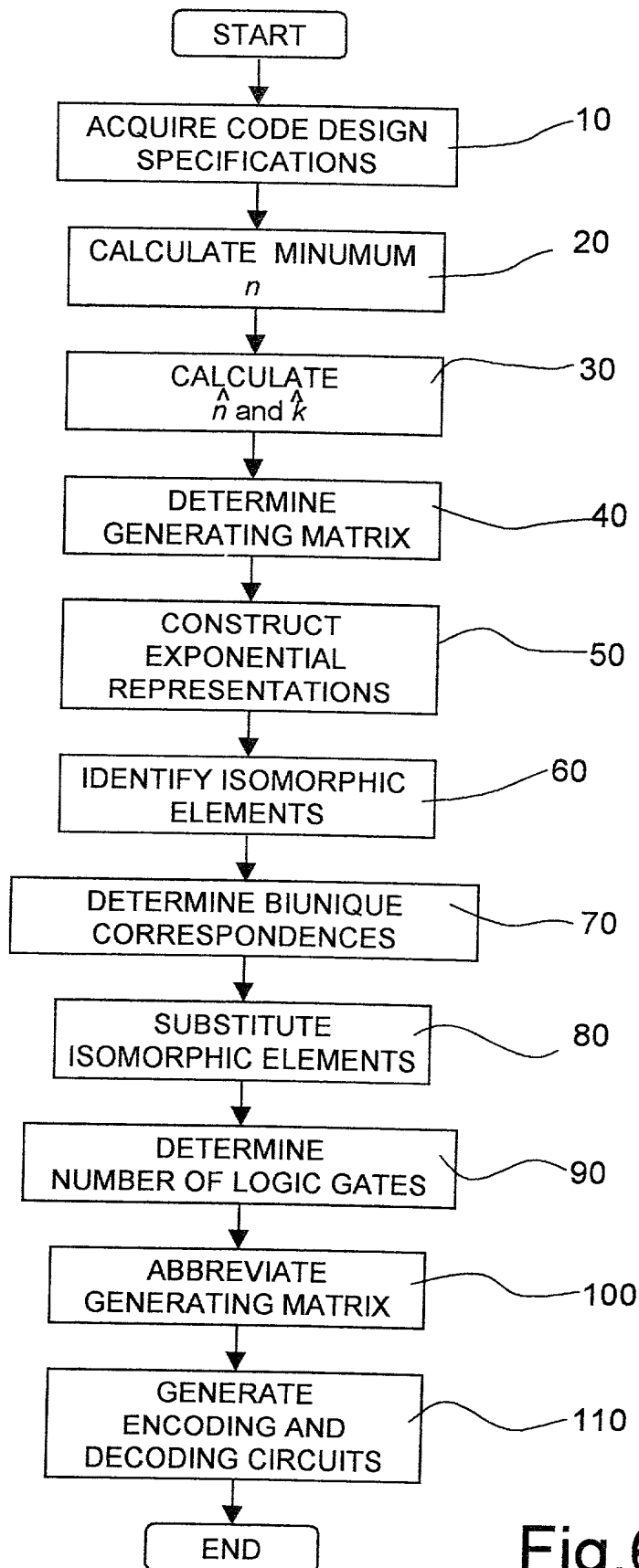


Fig.6

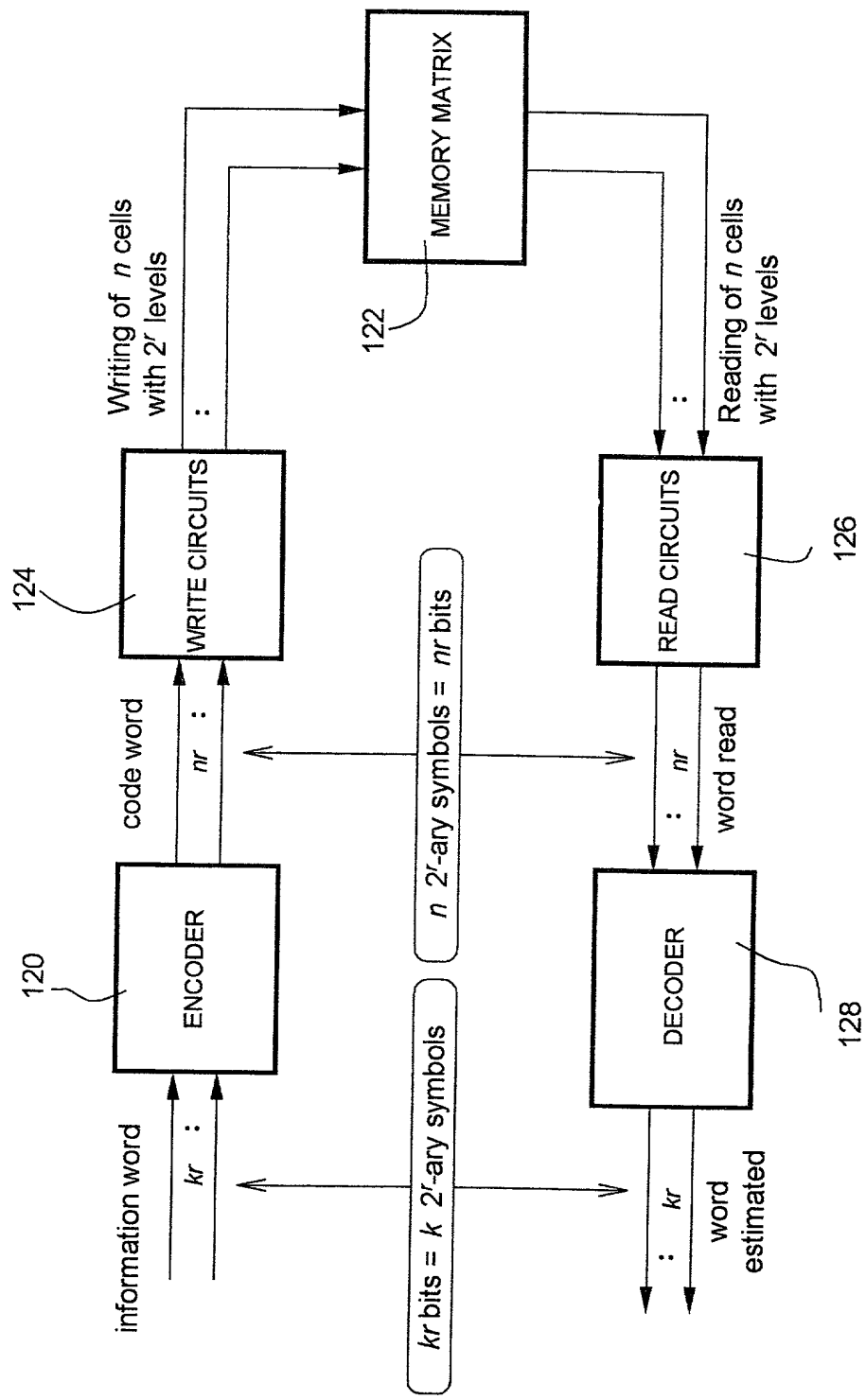


Fig. 7

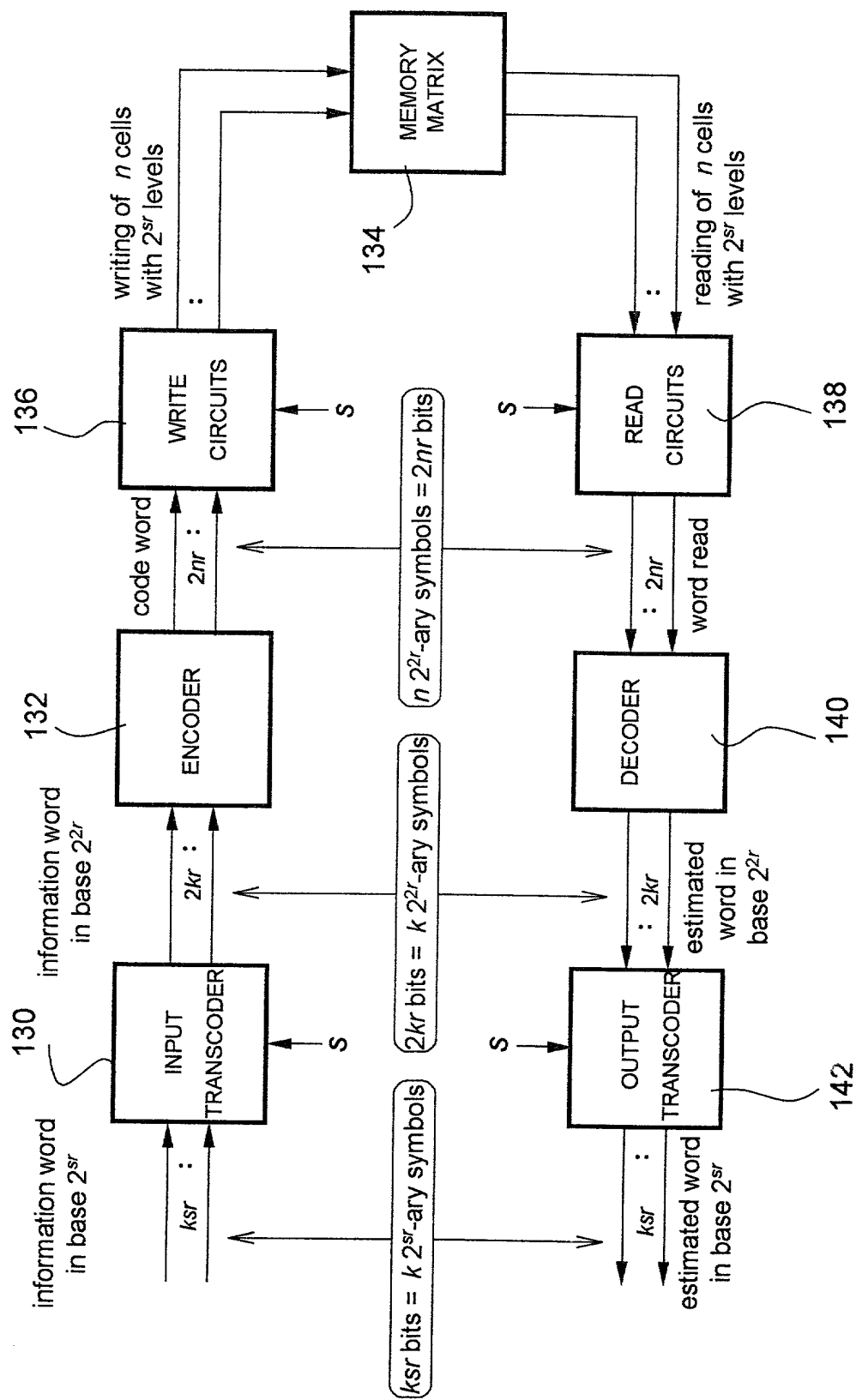


Fig. 8